ABSTRACT

Pre-authentication information of devices is used to securely authenticate arbitrary peer-to-peer ad-hoc interactions. In one embodiment, public key cryptography is used in the main wireless link with location-limited channels being initially used to pre-authenticate devices. Use of public keys in the pre-authentication data allows for the broadening of types of media suitable for use as location-limited channels to include, for example, audio and infrared. Also, it allows a range of key exchange protocols which can be authenticated in this manner to include most public-key-based protocols. As a result, a large range of devices, protocols can be used in various applications. Further, an eavesdropper is forced to mount an active attack on the location-limited channel itself in order to access an ad-hoc exchange. However, this results in the discovery of the eavesdropper.